II. CLAIM AMENDMENTS

1. (Previously Presented) A method in a mobile system in a mobile system, comprising :

encrypting data to be transmitted between a radio access network of a packet-switched time division multiple access mobile system and user equipment using an encryption algorithm at a transmitting end,

wherein an encryption algorithm of a radio access network of a wideband code division multiple access mobile system is used as the encryption algorithm, in which case input parameters of a format required by the encryption algorithm are created on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

2. (Previously Presented) A method as claimed in claim 1 or 49, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

3. (Currently Amended) A method as claimed in claim ~~1 or~~ 2, wherein the encryption algorithm is a black box and implementation of the encryption algorithm is exactly the same in both the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system.

4. (Original) A method as claimed in claim 1, wherein the input parameters comprise a counter parameter.

5. (Previously Presented) A method as claimed in claim 4, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of a second layer signaling plane or other data.

6. (Previously Presented) A method as claimed in claim 1 or 49, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

7. (Previously Presented) A method as claimed in claim 4, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

8. (Previously Presented) A method as claimed in claim 7, wherein the extended TDMA frame number is based on extending a T1 counter part of GSM.

9. (Previously Presented) A method as claimed in claim 7, wherein information on a last used extended TDMA frame number is stored in the user equipment for a next connection.

10. (Original) A method as claimed in claim 9, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and before the information is used

in a new radio connection to form an extended TDMA frame number, the value of the number formed by said most significant bits is increased by one.

11. (Previously Presented) A method as claimed in claim 4, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises a time slot number.

12. (Previously Presented) A method as claimed in claim 4, wherein when executing the encryption algorithm in an RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

13. (Previously Presented) A method as claimed in claim 12, wherein information is stored on a last used hyper frame number in the user equipment for a next connection, and before the information is used in a new radio connection to form a hyper frame number, the value of the number is increased by one.

14. (Previously Presented) A method as claimed in claim 13, wherein the information to be stored on the last used hyper frame number comprises a certain number of most significant bits of the hyper frame number.

15. (Previously Presented) A method as claimed in claim 1 or 49, wherein when a connection of the user equipment changes between the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system, information on a last used extended TDMA frame number or hyper frame number is provided to a new

radio access network, and the same encryption key input parameter as in an old radio access network is used as the encryption key input parameter of the encryption algorithm in the new radio access network.

16. (Original) A method as claimed in claim 15, wherein the information to be provided comprises a certain number of most significant bits, and before the information is used in a new radio access network, the value of the number formed by said most significant bits is increased by one.

17. (Previously Presented) An apparatus for a mobile system, comprising:

means for encrypting data to be transmitted of a packet-switched time division multiple access mobile system using an encryption algorithm,

wherein the encryption algorithm is an encryption algorithm of a radio access network of a wideband code division multiple access mobile system, and the user equipment comprises means for creating input parameters of agreed format required by the encryption algorithm on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

18. (Currently Amended) An apparatus as claimed in claim 17 ~~and~~ or 50, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

19. (Previously Presented) An apparatus as claimed in claim 17, wherein the encryption algorithm is a black box and implementation of the encryption algorithm is exactly the same in both the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system.

20. (Original) User equipment as claimed in claim 17, wherein the input parameters comprise a counter parameter.

21. (Previously Presented) User equipment as claimed in claim 20, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of a second layer signaling plane or other data.

22. (Currently Amended) User equipment as claimed in claim 17 ~~and~~ or 50, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

23. (Previously Presented) User equipment as claimed in claim 20, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

24. (Previously Presented) User equipment as claimed in claim 23, wherein the extended TDMA frame number is based on extending a T1 counter part of GSM.

25. (Previously Presented) User equipment as claimed in claim 23, wherein the user equipment comprises means for storing information on a last used extended TDMA frame number for a next connection.

26. (Original) User equipment as claimed in claim 25, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio connection to form an extended TDMA frame number.

27. (Previously Presented) User equipment as claimed in claim 20, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises a time slot number.

28. (Previously Presented) User equipment as claimed in claim 20, wherein when executing the encryption algorithm in an RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

29. (Previously Presented) User equipment as claimed in claim 28, wherein the user equipment comprises means for storing information on a last used hyper frame number for a next connection.

30. (Original) User equipment as claimed in claim 29, wherein the information to be stored on the last used hyper frame number comprises a certain number of the most

significant bits of the hyper frame number, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio connection to form a hyper frame number.

31. (Currently Amended) User equipment as claimed in claim 17 ~~and~~ or 50, wherein the user equipment comprises means for providing information on a last used extended TDMA frame number or hyper frame number to a new radio access network when a connection of the user equipment changes between the radio access network of a packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system, and for using the same encryption key parameter as in an old radio access network as the encryption key parameter of the encryption algorithm in the new radio access network.

32. (Original) User equipment as claimed in claim 31, wherein the information to be provided comprises a certain number of most significant bits, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio access network.

33 – 46 (Cancelled)

47. (Currently Amended) The apparatus as claimed in claim ~~17 or~~ 18, wherein the apparatus is a packet-switched time division multiple access mobile system and comprises means for receiving information on a last used extended TDMA frame number or hyper frame number to the user equipment when a connection of the user equipment changes between the radio access network of the packet-switched time

division multiple access mobile system and the radio access network wideband code division multiple access mobile system, and for using as the encryption key parameter of the encryption algorithm, the encryption key parameter according to the received information.

48. (Previously Presented) The apparatus as claimed in claim 47, wherein the information to be provided comprises a certain number of most significant bits, and the radio access network of the packet-switched time division multiple access mobile system comprises means for increasing by one the value of the number formed by said most significant bits before the information is used.

49. (Previously Presented) A method in a mobile system, comprising:

decrypting received data, transmitted between a radio access network of a packet-switched time division multiple access system and user equipment, using an encryption algorithm at the receiving end,

using an encryption algorithm of a radio access network of a wideband code division multiple access mobile system as the encryption algorithm; and

creating input parameters of a format required by the encryption algorithm on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

50. (Previously Presented) An apparatus for a mobile system, comprising:

means for decrypting data received using an encryption algorithm at a receiving end wherein the encryption algorithm is an encryption algorithm of a radio access network of a packet switched time division multiple access mobile system employing a wideband code division multiple access method of a universal mobile telecommunications system;

means for creating input parameters of a format required by the encryption algorithm on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

51. (Previously Presented) The apparatus of claim 18 ~~and 50~~ wherein the apparatus is a user equipment UE.

52. (Previously Presented) The apparatus of claim 18 ~~and 50~~ wherein the apparatus is a GPRS/EDGE radio access network GERAN.

53. (New) The apparatus of claim 50 wherein the apparatus is a user equipment UE.

54. (New) The apparatus of claim 50 wherein the apparatus is a GPRS/EDGE radio access network GERAN.